## IN THE CLAIMS

Please amend the claims as follows:

1.    (currently amended) A method of managing passwords for a plurality of ~~system resources~~ software tools accessible by a user, said method comprising:

providing a password registry for storing passwords within ~~plurality of front-end interfaces on~~ a workstation, ~~each of said front-end interfaces corresponds to a type of system resource accessible by a user via said workstation~~;

allowing each of a plurality of software tools to register its password in said password registry via a respective one of a plurality of front-end processes within said workstation, wherein each said password is encrypted by said respective front-end process before being stored in said password registry ~~generating an encrypted password for each of said types of system resources from encrypting a corresponding unencrypted password provided by a user~~;

~~storing said encrypted passwords in a password registry within said workstation;~~

in response to an access request to one of said ~~system resources~~ software tools via a corresponding one of said front-end processes ~~interfaces~~, determining if ~~retrieving from said password register~~ an encrypted password ~~corresponding to~~ associated with said requested ~~system resource~~ software tool is stored in said password registry; ~~and~~

in a determination that said encrypted password associated within said software tool is stored in said password registry, sending ~~passing~~ said ~~retrieved~~ encrypted password from said password registry to said corresponding front-end process ~~interface~~ for decryption in order to permit said access request; and

in a determination that said encrypted password associated within said software tool is not stored in said password registry, notifying said front-end process to prompt for a password from a user.

2.    (previously presented) The method of claim 1, wherein said method further includes associating each of said encrypted passwords with an identifying information.

3.    (previously presented) The method of claim 2, wherein said identifying information includes at least one of a user ID, a resource hostname, and a resource type.

4.    (currently amended) The method of claim 3, wherein said method further includes utilizing at least one of said user ID, said resource hostname, and said resource type as a query key to uniquely identify said each ~~system resource~~ software tool and ~~said~~ its associated encrypted password ~~for said each system resource~~.

5.    (previously presented) The method of claim 4, wherein said method further includes retrieving a corresponding one of said encrypted passwords using said query key.

6-25.  canceled

26.   (currently amended) A computer readable medium having computer program product for managing passwords for a plurality of ~~system resources~~ software tools accessible by a user, said computer readable medium comprising:

    computer program code for providing a password registry for storing passwords within ~~plurality of front-end interfaces on~~ a workstation~~, each of said front-end interfaces corresponds to a type of system resource accessible by a user via said workstation~~;

computer program code for <u>allowing each of a plurality of software tools to register its password in said password registry via a respective one of a plurality of front-end processes within said workstation, wherein each said password is encrypted by said respective front-end process before being stored in said password registry</u> ~~generating an encrypted password for each of said types of system resources from encrypting a corresponding unencrypted password provided by a user~~;

~~computer program code for storing said encrypted passwords in a password registry within said workstation;~~

computer program code for, in response to an access request to one of said ~~system resources~~ <u>software tools</u> via a corresponding one of said front-end <u>processes</u> ~~interfaces~~, <u>determining if</u> ~~retrieving from said password register~~ an encrypted password ~~corresponding to~~ <u>associated with</u> said requested ~~system resource~~ <u>software tool is stored in said password registry</u>; ~~and~~

computer program code for<u>, in a determination that said encrypted password associated within said software tool is stored in said password registry, sending</u> ~~passing~~ said ~~retrieved~~ <u>encrypted</u> password from said password registry to said corresponding front-end <u>process</u> ~~interface~~ for decryption in order to permit said access request<u>; and</u>

<u>computer program code for, in a determination that said encrypted password associated within said software tool is not stored in said password registry, notifying said front-end process to prompt for a password from a user.</u>

27.    (previously presented) The computer readable medium of claim 26, wherein said computer readable medium further includes computer program code for associating each said encrypted password with an identifying information.

28.    (previously presented) The computer readable medium of claim 27, wherein said identifying information includes at least one of a user ID, a resource hostname, and a resource type.

29.    (currently amended) The computer readable medium of claim 28, wherein said computer readable medium further includes computer program code for utilizing at least one of said user ID, said resource hostname, and said resource type as a query key to uniquely identify said each ~~system resource~~ software tool and ~~said~~ its associated encrypted password ~~for said each system resource~~.

30.    (previously presented) The computer readable medium of claim 29, wherein said computer readable medium further includes computer program code for retrieving a corresponding one of said encrypted passwords using said query key.